AMENDMENT TO THE CLAIMS

Please amend the claims as follows:

1. (Currently amended) A method for updating [[an inherent key-encrypted]] a program in a system including an LSI device and an external memory, [[the inherent key-encrypted program being generated by encryption with an inherent key unique to the LSI device and being stored in the external memory,]] the method comprising:

a step of transmitting by the system an inherent ID of the LSI device and an application ID which is identification information of an update object program to a server;

a step of determining by the server whether or not the update object program may be transmitted based on the transmitted inherent ID and application ID, and transmitting by the server additional information of the update object program if it is determined that the update object program may be transmitted;

a step of determining by the system whether or not program update is possible based on the transmitted additional information, and requesting by the system the server to transmit a common key-encrypted program generated by encryption with a common key if it is determined that program update is possible;

a [[first]] step of receiving by the system the common key-encrypted program transmitted from the server;

a [[second]] step of decrypting by the system the received common key-encrypted program to generate a raw program; and

a [[third]] step of re-encrypting by the system the raw program with [[the]] an inherent key unique to the LSI device and storing the re-encrypted program in the external memory as a new inherent key-encrypted program.

2. (Currently amended) The program update method of claim 1, further comprising the steps of:

receiving by the system common key information transmitted from the server; and

generating by the system a raw common key using the received common key information,

wherein at the [[second]] decrypting step, the raw common key is used to decrypt the common key-encrypted program.

3. (Original) The program update method of claim 2, wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key.

4. (Currently amended) The program update method of claim 1, wherein:

the LSI device includes an internal memory in which inherent key information is stored;

the system uses the inherent key information stored in the internal memory to generate a raw inherent key at boot-up of the system; and

at the [[third]] re-encrypting step, the raw inherent key is used for re-encrypting the raw program.

5. (Original) The program update method of claim 4, wherein the inherent key information includes an encrypted inherent key generated by encrypting the raw inherent key with a raw third intermediate key and an encrypted second intermediate key generated by

encrypting the raw third intermediate key with a raw fourth intermediate key.

6. (Original) The program update method of claim 4, wherein the generated raw inherent key is stored in a register of the LSI device and is used for decrypting the inherent key-encrypted program to a raw program for execution of the inherent key-encrypted program.

7. (Original) The program update method of claim 1, wherein:

the LSI device includes a boot ROM in which a boot program is stored;

the external memory includes an acquisition program for establishing data transmission between the LSI device and a server; and

the system executes reception of the common key-encrypted program based on the acquisition program stored in the external memory, and controls update processing performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM.

8. (Currently amended) The program update method of claim 1, further comprising the step of receiving a HASH value of the raw program transmitted from the server,

wherein at the [[second]] decrypting step, the received HASH value is used to perform a HASH verification on the decrypted raw program.

9-11. (Cancelled)